Claim Amendments

Claim 1 (previously presented): A system to establish a trusted and decentralized peer-to peer network comprising:

communication means;

n user computing devices connected to the communication means, where n is greater than or equal to 1 and is an integer; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communications network with at least 2 of the n user computing devices through which digital signals are shared securely between the host computing device and the 2 user computing devices of the trusted communications network, the host computer sending a public key to a first of the 2 user computing devices and the first user computing device sending the public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network.

Claim 2 (previously presented): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

receiving the public key at the second user computing device to establish a decentralized trusted communications network between the host computing device, the first and the second computing device through which digital signals are shared securely between the host computing device, the first user computing device and the second user computing device; and

sending digital signals directly from the first user computing device securely to the second user computing device.

Claim 3 (previously presented): A method as described in Claim 2 including the step of creating encryption and decryption keys.

Claim 4 (previously presented): A method as described in Claim 3 including the step of creating a searchable ciphertext file containing identifiable network information on each computing device.

Claim 5 (previously presented): A method as described in Claim 4 wherein the creating step includes the step of creating a searchable ciphertext file containing identifiable network information on each computing device which is shared with every other computing device.

Claim 6 (previously presented): A method as described in Claim 5 including the step of finding by a member of the trusted peer-to-peer network other members of the trusted peer-to-peer network.